**计算机科学与技术学院2017-2018学年第2学期 考试试卷**

信息安全数学基础 A卷 闭卷

姓名\_\_\_\_\_\_\_\_\_\_\_\_班级\_\_\_\_\_\_\_\_\_\_\_\_学号\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_考试日期 2018-6-2

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 题号 | 一 | 二 | 三 | 四 | 总分 | 核对人 |
| 题分 | 20 | 20 | 35 | 25 | 100 |  |
| 得分 |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **证明题(本大题3小题，共20分)** |
|  |  |

1. 若与为不同的素数，，整数满足，且，试证明：与两者中有且仅有一个整数是的因子。（6分）
2. 设是两个正整数，，试证明：不能表示成为正整数)的形式.（6分）
3. 设素数，，试证明。（8分）

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **计算题(本大题2小题，共20分)** |
|  |  |

1. 计算，结果取最小非负剩余。（10分）
2. 计算勒让德符号。（10分）

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **解方程或方程组(本大题3小题，共35分)** |
|  |  |

1. 求解同余式.（10分）
2. 求解同余式组.(10分)
3. 求解同余式（15分）.

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **解答题(本大题2小题，共25分)** |
|  |  |

1. 试判断44是否为模117的21次剩余。（10分）
2. 设是上的多项式，是在的扩域上的一个根，

（1）试证明是上的不可约多项式。（5分）

（2）试判断是否是的8元子域中的元素，并说明理由。（5分）

（3）试求在上的极小多项式。（5分）